Introducción a la Teoría de Códigos

M.A. García, L. Martínez, T. Ramírez

Facultad de Ciencia y Tecnología. UPV/EHU

Resumen Teórico
Apartado 1 del Tema 3:
Definición y primeras propiedades

Mayo de 2017

1 Definición y primeras propiedades

Tanto en este tema como en el siguiente, nos vamos a centrar en los códigos de bloque de longitud n sobre $\mathbb{F}_q$. Esto es, trabajaremos con $C \subseteq \mathbb{F}_q^n$. Para seguir la notación introducida en el tema anterior los elementos de $\mathbb{F}_q^n$ se denotarán por $x_1 \dots x_n$, siendo $x_i \in \mathbb{F}_q$ para $i = 1, \dots, n$, salvo que pueda inducir a error. En tal caso, esto es, cuando pueda inducir a error la notación anterior, se empleará la notación habitual de los elementos de $\mathbb{F}_q^n$: $(x_1, \dots, x_n)$.

Sabemos que $\mathbb{F}_q^n$ es un $\mathbb{F}_q$-espacio vectorial de dimensión n con la suma y la multiplicación por un escalar habitual. Es por ello que, de entre los subconjuntos de $\mathbb{F}_q^n$, nos fijaremos en aquellos que posean alguna estructura algebraica detrás. En concreto, en este tema nos centraremos en el estudio de los códigos conocidos como códigos lineales, que definimos a continuación:

Definición Sea $C \subseteq \mathbb{F}_q^n$. Se dice que C es un **código lineal**, si C es un subespacio vectorial de $\mathbb{F}_q^n$.

Observamos que si $C \subseteq \mathbb{F}_q^n$ es un código lineal, entonces por ser un subespacio vectorial de $\mathbb{F}_q^n$ se verifica:

1. $0 \dots 0 \in C$.
2. Si $\mathbf{x}, \mathbf{y} \in C$, entonces $\mathbf{x}+\mathbf{y}, \mathbf{x}\text{-}\mathbf{y} \in C$.
3. Existe una base $\{\mathbf{x}_1, \dots, \mathbf{x}_k\}$ de C, siendo $k \leq n$. Además, dado $\mathbf{y} \in C$, existen unos únicos escalares $(\alpha_1, \dots, \alpha_k) \in \mathbb{F}_q^k$ tales que $\mathbf{y} = \sum_{i=1}^{k} \alpha_i \mathbf{x}_i$.
4. Si la dimensión de C es k, entonces $|C| = q^k$.

Si $C \subseteq \mathbb{F}_q^n$ es código lineal de dimensión k, le llamaremos de forma breve (n, k)-código.

Nos interesa ver si podemos calcular de forma sencilla la distancia mínima de un código lineal. Al estar trabajando en $\mathbb{F}_q^n$, lo primero que vemos es que podemos relacionar $d(\mathbf{x}, \mathbf{y})$ con el peso de otra palabra de $\mathbb{F}_q^n$. En concreto, se puede probar

Lema 1.1 *Sean $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^n$. Entonces, $d(\boldsymbol{x}, \boldsymbol{y}) = w(\boldsymbol{x} - \boldsymbol{y})$.*

Este lema nos va a servir para tener otra forma de calcular la distancia mínima de un código lineal, tal y como se establece en la siguiente proposición:

Proposición 1.2 *Sea $C \subseteq \mathbb{F}_q^n$ un código lineal con distancia mínima d y peso mínimo w. Entonces, $d = w$.*

Este resultado va a facilitar enormemente el cálculo de la distancia mínima de un (n,k)-código C sobre $\mathbb{F}_q$, porque en lugar de tener que calcular las distancias de $\binom{q^k}{2}$ pares de palabras de C distintas y luego determinar su mínimo, solamente necesitaremos calcular los pesos de q^k-1 palabras de C no nulas.

Ejemplo El código binario

$$\begin{aligned} C \quad = \{&0000000, 0110100, 0011010, 0001101,\\ &1000110, 1001011, 1011100, 0010111,\\ &1010001, 1110010, 011100, 1111111,\\ &0101110, 1101000, 0100011, 1100101\} \end{aligned}$$

es un código lineal de dimensión 4,¡ ya que una base de este código lineal es

$$\{1000110, 0110100, 0011010, 0001101\}.$$

Aplicando la Proposición 1.2, deducimos que la distancia mínima de C es 3, ya que este valor es el peso mínimo de C.